

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75787 A1

- (51) International Patent Classification⁷: G06F 12/14, H04L 9/00
Jugong Apt. 408-504, 7, Byalyang-dong, Kwacheon-si, Kyungki-do 427-040 (KR).
- (21) International Application Number: PCT/KR99/00277
(81) Designated States (*national*): JP, KR, US.
- (22) International Filing Date: 5 June 1999 (05.06.1999)
(84) Designated States (*regional*): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
- (25) Filing Language: English
Published:
— With international search report.
- (26) Publication Language: English
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
- (71) Applicant and
(72) Inventor: PARK, Hyo, Joon [KR/KR]; Kwacheon



WO 00/75787 A1

(54) Title: DIGITAL PRODUCT LICENSE CONTROL SYSTEM BASED ON INDEPENDENT DIGITAL PRODUCT REGISTRATION SERVER

(57) Abstract: The registration server is independent of digital product manufacturers and open to all digital product manufacturers. The manufacturer registers his digital product to the server and gets product registration file of the product from the server. The product manufacturer merges the product and the product registration file and encrypts them using manufacturer digital product license control program. If a public digital product is executed on user computer, said digital product is linked to digital product execution program which is subsystem of user digital product license control program. The program decrypts said digital product and reads the product ID from the product registration file and checks the license file received from a digital product registration server. If there is no license for the digital product, said program asks the user to buy a license of the product.

Title of invention

Digital product license control system based on independent digital product registration server

Technical field

Digital product license control

Background art

Software license control, digital product license control, cryptography

Publication – Garfinkel, Simson. PGP(Pretty Good Privacy).

Schneier, Bruce. Applied Cryptography

Disclosure of invention

The registration server is independent of digital product manufacturers and open to all digital product manufacturers. Every digital product needs to be modified to participate in this new digital product license control system. The digital product manufacturer is registered to the registration server. Normally such digital products as MP3 or VOD files, which cannot be

2

executed alone, are processed by specific programs (players). The manufacturer registers his digital product, with the player information, to the server and gets product registration file of the product from the server. The product manufacturer merges the product and the product registration file and encrypts them using manufacturer digital product license control program. The output is the format of public digital product. Public digital product has specific file type such as "sampleMP3.ds1". If a public digital product is executed on user computer, said digital product is linked to digital product execution program which is subsystem of user digital product license control program. Normally digital products are downloaded from Internet and are executed by double clicking. Upon double clicking of the digital product, the digital product execution program processes the digital product. The program decrypts said digital product and reads the product ID from the product registration file. And said program checks the license file to know whether there is usage license for said digital product. The license file was received from a digital product registration server. If there is no license for the digital product, said program asks the user to buy a license of the product. If user doesn't buy it, said program stops the running of the digital product. If the user buys it, the program receives new license file, which includes the purchased license, from the server and the program changes the digital product to a personal digital product format. Personal digital product has specific file type such as "sampleMP3.ds2". If there is

the license, the program can change the public digital product to a personal digital product any time. Personal digital product cannot be interpreted without the user-ID file which was used in creating said personal digital product. The program calls player to execute personal digital product. Unauthorized user cannot use the personal digital product. Also the license file cannot be used by unauthorized user because said file is encrypted by the user public key and digital signed by the secret key of a digital product registration server. To use a license file, user needs the secret key of the user and needs passphrase to activate the secret key. The license file is digital signed by digital product registration server and cannot be modified by a user to add unauthorized license. The license file includes 3 information in addition to license information. They are user ID, CPU ID and owner ID. If user ID in license file is different from user ID of user-ID file, the license file is ignored by user digital product license control program. If CPU ID in license file is different from CPU ID of the processor, such as PSN of Intel processor Pentium III, the license file is ignored by user digital product license control program. So, even authorized user cannot execute personal digital product on unauthorized computers.

All digital product manufacturers register their products to the central digital product registration server. The central registration server distributes the registered product information to digital product registration servers all over the world. 3 types of registration need to be done by user. User registration,

CPU registration and digital product usage license registration. User does user registration for himself once per person. After that, the user registers his CPU once per CPU. User registers digital product usage license once per every product of specific CPU. All the registration is done after the connection to a digital product registration server. On user registration, the user gets partial user-ID file from the digital product registration server. After receiving the partial user-ID file, user digital product license control program attaches public/secret key pair of the user and public key of the registration server of the user to the partial user-ID file. This user-ID file is essential in registering CPU and purchasing digital product. The user-ID file is independent of any CPU and this file needs to be copied to all of his CPUs. On CPU registration, user gets license file from digital product registration server. And the license file is updated every time the user purchases new digital product or upgrades a digital product. The digital product information is added to the license file every time new product is purchased or a product is upgraded. Also because of expiration date, the license file is refreshed periodically. Expiration date or refresh period prevents unauthorized long-term use of the user-ID file or license file. Digital product usage license is given to a specific CPU of a specific user. In addition to direct purchase through public digital product execution, there is a indirect purchase. To purchase a digital product without executing the public digital product, user selects product category on license control

program screen, and then selects the digital product on displayed relevant digital products in that product category. Then, the user license control program sends digital product purchase request to the digital product registration server. The license file is dependent on a specific CPU. The license file is given to a specific CPU of a specific user. Both the user-ID file and license file is encrypted by user public key and digital signed by digital product registration server secret key. So, only the registration server can modify said files. In addition to above method – called user/CPU based license, there are two more methods. One is user-based license. The license is given to a specific user without having any CPU restriction on its license file. This license can be used on any CPU and strongly controlled by the user. The other method is CPU-based license. The license is given to a specific CPU without having any user restriction on its license file.

Normally license file is encrypted by user public key but CPU based license file is encrypted by the CPU public key. For CPU based license, one pair of secret/public key is created just for the CPU. In case of User/CPU based license and user based license, the pair of secret/public key of the user is used without creating new key pair for the CPU. In case of company, there is an owner in addition to an user of a PC/workstation. This owner has right to change the user of a PC/workstation. If an employee quits the company, the company (owner) is to assign new user to the PC/workstation. There is owner information in addition to user information in license file. If digital

product is executed on a specific machine such as MP3 player, which doesn't have such full configuration as personal computer, the digital product needs to be purchased on a computer and to be transferred to said machine. The user needs to move his user-ID file, license file and personal digital products to said machine. Said user-ID file, license file are simplified ones and created by user digital license control program. Basically said machine is treated as part of the computer which has the license file. Said machine has no CPU ID and is treated as if said machine has same CPU ID as said computer. If a user of said machine doesn't have a computer, it can be done on any computer. User digital license control program provides the way to create user-ID file and license file for said machine.

Best mode for carrying out the invention

Method of digital product license control based on independent digital product registration server comprising the steps of:

- . creating secret/public key pair for a digital product manufacturer by the manufacturer digital product license control program on the manufacturer computer.
- . connecting central digital product registration server, sending said manufacturer's public key to said registration server and receiving the

public key of said registration server.

. registering manufacturer once per manufacture to the central digital product registration server and receiving partial user-ID file from digital product registration server. Manufacturer digital product license control program attaches the manufacturer secret/public key pair and the public key of central digital product registration server to the partial user-ID file that includes manufacturer information encrypted by manufacturer public key and digital signed by the sever secret key.

. registering digital product, with player information, to central digital product registration server and receiving product registration file of the product from the server.

. distributing the product information to all digital product registration servers in the world by central digital product registration server. Registered digital product information includes product ID, price, player name, etc. So, user can select digital product from the registered digital product list. It is easier for user to buy a digital product by double clicking the public digital product and following the instruction given by the user digital product execution program.

. merging the product and said product registration file and encrypting them by manufacturer digital product license control program. The output is the format of public digital product.

. creating secret/public key pair for a user by the user digital product license

control program on the user computer.

. connecting digital product registration server by selecting one from the digital product registration server list, sending said user's public key to said registration server and receiving the public key of said registration server.

. registering user once per person to the digital product registration server and receiving partial user-ID file from digital product registration server.

User digital product license control program attaches the user secret/public key pair and the public key of the user's digital product registration server to the partial user-ID file that includes user information encrypted by user public key and digital signed by the server secret key. This user-ID file is essential in registering CPU and in registering digital product usage license.

. registering CPU for his computer hardware once per CPU to said digital product registration server and receiving license file that includes CPU information encrypted by user public key and digital signed by digital product registration server secret key.

. downloading public digital products from Internet by user

. double clicking public digital product on user computer.

. linking said digital product to digital product execution program of user digital product license control program.

. processing public digital product, decrypting said public digital product and reading the product ID from the product registration file by the linked digital product execution program.

- . checking the license file to know whether there is usage license for said digital product.
- . buying a license for the product or stopping the process, if there is no license for the digital product.
- . receiving new license file which includes the purchased license.
- . changing the digital product to a personal product format if there is license.
- . calling player to execute personal digital product
- . storing user information, CPU information and digital product usage license information in digital product registration server database by the server.
- . replicating digital product registration server database to central digital product registration server database for backup purpose and for cross digital product registration server function such as the change of digital product registration server and change of user who is registered to a different digital product registration server from the former user.
- . updating user-ID file and license file based on expiration date or refresh period by user. Expiration date or refresh period prevents unauthorized long-term use of the user-ID file or license file.
- . changing the user of a CPU by the owner of the CPU in case of user change. License file has owner information.

Industrial applicability

Digital product license control system works based on following servers and software packages:

- . Central digital product registration server gets digital product information from all digital product manufacturers and distributes the registered product information to digital product registration servers all over the world. Said central registration server does the interface between all digital product manufacturers and digital product registration centers.
- . Normal digital product registration servers give user the digital product information that is given by central digital product registration server, get registration request from users and give license file to users.
- . Software packages for general users, normal digital product registration servers, central digital product registration server and digital product manufacturers.

What is claimed is:

1. Method of digital product license control based on independent digital product registration server comprising the steps of:

- . creating secret/public key pair for a digital product manufacturer by the manufacturer digital product license control program on the manufacturer computer.
- . connecting central digital product registration server, sending said manufacturer's public key to said registration server and receiving the public key of said registration server.
- . registering manufacturer once per manufacture to the central digital product registration server and receiving partial user-ID file from digital product registration server. Manufacturer digital product license control program attaches the manufacturer secret/public key pair and the public key of central digital product registration server to the partial user-ID file that includes manufacturer information encrypted by manufacturer public key and digital signed by the sever secret key.
- . registering digital product, with player information, to central digital product registration server and receiving product registration file of the product from the server.
- . distributing the product information to all digital product registration

servers in the world by central digital product registration server. Registered digital product information includes product ID, price, player name, etc. So, user can select digital product from the registered digital product list. It is easier for user to buy a digital product by double clicking the public digital product and following the instruction given by the user digital product execution program.

. merging the product and said product registration file and encrypting them by manufacturer digital product license control program. The output is the format of public digital product.

. creating secret/public key pair for a user by the user digital product license control program on the user computer.

. connecting digital product registration server by selecting one from the digital product registration server list, sending said user's public key to said registration server and receiving the public key of said registration server.

. registering user once per person to the digital product registration server and receiving partial user-ID file from digital product registration server.

User digital product license control program attaches the user secret/public key pair and the public key of the user's digital product registration server to the partial user-ID file that includes user information encrypted by user public key and digital signed by the sever secret key. This user-ID file is essential in registering CPU and in registering digital product usage license.

. registering CPU for his computer hardware once per CPU to said digital

product registration server and receiving license file that includes CPU information encrypted by user public key and digital signed by digital product registration server secret key.

- . downloading public digital products from Internet by user
- . double clicking public digital product on user computer.
- . linking said digital product to digital product execution program of user digital product license control program.
- . processing public digital product, decrypting said public digital product and reading the product ID from the product registration file by the linked digital product execution program.
- . checking the license file to know whether there is usage license for said digital product.
- . buying a license for the product or stopping the process, if there is no license for the digital product.
- . receiving new license file which includes the purchased license.
- . changing the digital product to a personal product format if there is license.
- . calling player to execute personal digital product
- . storing user information, CPU information and digital product usage license information in digital product registration server database by the server.
- . replicating digital product registration server database to central digital product registration server database for backup purpose and for cross digital product registration server function such as the change of digital product

registration server and change of user who is registered to a different digital product registration server from the former user.

. updating user-ID file and license file based on expiration date or refresh period by user. Expiration date or refresh period prevents unauthorized long-term use of the user-ID file or license file.

. changing the user of a CPU by the owner of the CPU in case of user change. License file has owner information.

2. A method according to claim 1 wherein connecting to the only one digital product registration server automatically. Only one registration server exists in the world and does all registration service.

Consequently, there is no replication from registration server to central registration server and no distribution of registered product information from central registration server to registration servers, since there is only one server.

3. A method according to claim 1 wherein validating digital product usage license without giving limitation to a specific CPU. User digital product license control program on user computer doesn't check CPU information if "user based license" indicator is on in license file.

4. A method according to claim 1 wherein validating digital product usage license without giving limitation to the specific user described in license file.

User digital product license control program on user computer doesn't check user information if "CPU based license" indicator is on in license file. Instead of entering "user passphrase" user enters "passphrase of the CPU". In registering CPU for the computer once per CPU, user digital product license control program creates secret/public key pair for the CPU and sends the public key to digital product registration server. The license file is encrypted by the CPU public key and digital signed by digital product registration server

5. A method according to claim 1 wherein transferring user-ID file, license file and personal digital products to a specific machine such as MP3 player. If digital product is executed on said machine, which doesn't have such full configuration as personal computer, the digital product needs to be purchased on a computer and to be transferred to said machine. Said user-ID file, license file are simplified ones and created by user digital license control program. Basically said machine is treated as part of the computer which has the license file. Said machine has no CPU ID and is treated as if said machine has same CPU ID as said computer. If a user of said machine doesn't have a computer, it can be done on any computer. User digital license control program provides the way to create user-ID file and license file for said machine.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR 99/00277

CLASSIFICATION OF SUBJECT MATTER

IPC⁷: G 06 F 12/14; H 04 L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC⁷: G 06 F; H 04 L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, PAJ, EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98/42098 A1 (CRYPOWORKS) 29 April 1998 (29.04.98) totality. ----	

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

„A“ document defining the general state of the art which is not considered to be of particular relevance

„E“ earlier application or patent but published on or after the international filing date

„L“ document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

„O“ document referring to an oral disclosure, use, exhibition or other means

„P“ document published prior to the international filing date but later than the priority date claimed

„T“ later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

„X“ document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

„Y“ document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

„&“ document member of the same patent family

Date of the actual completion of the international search

6 April 2000 (06.04.2000)

Date of mailing of the international search report

31 July 2000 (31.07.2000)

Name and mailing address of the ISA/AT

Austrian Patent Office

Kohlmarkt 8-10; A-1014 Vienna

Facsimile No. 1/53424/535

Authorized officer

Fastenbauer

Telephone No. 1/53424/447

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR 99/00277

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
WO	A1	9842098	24-09-1998	AU	A1	67591/98	12-10-1998
				EP	A1	968585	05-01-2000